The Claims

1. (Original) One or more computer-readable media having stored thereon a plurality of instructions for generating a product identifier, wherein the plurality of instructions, when executed by one or more processors, causes the one or more processors to perform the following acts:

receiving a value;

padding the received value using a recognizable pattern;

converting the padded value to a number represented by a particular number of bits;

converting the number to an element of the Jacobian of a curve;

raising the element to a particular power;

compressing the result of raising the element to the particular power; and

outputting, as the product identifier, the compressed result.

2. (Original) One or more computer-readable media as recited in claim 1, wherein the receiving comprises receiving a numeric value associated with a copy of a product.

3. (Original) One or more computer-readable media as recited in claim 1, wherein the recognizable pattern comprises at least a portion of the received value.

4. (Original) One or more computer-readable media as recited in claim 1, wherein converting the padded value to a number represented by a particular number of bits comprises converting the padded value to a 114-bit number.

5. (Original) One or more computer-readable media as recited in claim 1, wherein converting the padded value to a number represented by a particular number of bits comprises:

defining a plurality of functions, wherein each of the plurality of functions returns a value that is a set of bits of a hash value generated based on an input value;

separating the padded value into a plurality of portions; and

using the plurality of portions as input values for the plurality of functions.

6. (Original) One or more computer-readable media as recited in claim 5, wherein each of the plurality of functions returns a set of least significant bits of a hash value generated based on the input.

7. (Original) One or more computer-readable media as recited in claim 5, wherein the hash value is generated using a secure hashing process.

8. (Original) One or more computer-readable media as recited in claim 5, wherein the set of bits includes a number of bits equal to half the particular number of bits.

9. (Original) One or more computer-readable media as recited in claim 5, wherein the separating comprises separating the padded value into two equal portions.

10. (Original) One or more computer-readable media as recited in claim 1, wherein the curve comprises a hyperelliptic curve.

11. (Original) One or more computer-readable media as recited in claim 1, wherein converting the number to an element of the Jacobian of the curve is based at least in part on an order of a group of points on the Jacobian of the curve, and wherein the order of the group of points on the Jacobian of the curve is maintained as a secret.

12. (Original) One or more computer-readable media as recited in claim 1, wherein the curve is given by the equation $y^2=f(x)$, wherein f(x) has a degree of $2 \cdot g+1$, and wherein g refers to the genus of the curve.

13. (Original) One or more computer-readable media as recited in claim 12, wherein converting the number to an element of the Jacobian of a curve comprises:

determining a value a(x), wherein the value a(x) is a monic irreducible polynomial of degree g;

determining a value b(x), wherein the value b(x) is a square root of f(x) modulo a(x) of degree less than a(x); and

using, as the element of the Jacobian of the curve, the values a(x) and b(x).

14. (Original) One or more computer-readable media having stored thereon a plurality of instructions that, when executed by one or more processors, causes the one or more processors to perform the following acts:

receiving a product identifier;

decompressing the product identifier to obtain a decompressed value;

raising the decompressed value to a particular exponent to obtain a resulting value, wherein the raising is based at least in part on an element of a Jacobian of a curve;

converting the resulting value to a number having a particular number of bits;

checking whether a set of bits of the particular number of bits represents a recognizable pattern; and

determining that the product identifier is valid if the set of bits do represent the recognizable pattern, and otherwise determining that the product identifier is invalid.

15. (Original) One or more computer-readable media as recited in claim 14, wherein the recognizable pattern comprises a duplicate of at least a portion of part of the resulting value.

16. (Original) One or more computer-readable media as recited in claim 14, wherein the curve comprises a hyperelliptic curve.

17. (Original) One or more computer-readable media as recited in claim 14, wherein the raising is further based at least in part on an order of a group of points on the Jacobian of the curve, and wherein the order of the group of points on the Jacobian of the curve is maintained as a secret.

18. (Original) One or more computer-readable media as recited in claim 14, allowing a software product associated with the product identifier to be installed only if the product identifier is determined to be valid.

19. (Original) One or more computer-readable media as recited in claim 14, wherein the plurality of instructions further causes the one or more processors to perform the following acts:

recovering another set of bits from the particular number of bits;

checking whether the other set of bits corresponds to a particular product; and

determining that authentication of the particular product succeeds if the other set of bits corresponds to the particular product, and otherwise determining that authentication of the particular product fails.

20. (Currently amended) A computerized method comprising:

receiving an encrypted product identifier;

recovering a plaintext message from the encrypted product identifier, wherein the recovering is based on a secret that is the size of a group of points on a Jacobian of a curve;

checking whether the plaintext message includes a particular value; and

determining that the encrypted product identifier is valid if the plaintext message includes the particular value, and otherwise determining that the encrypted product identifier is invalid.

21. (Original) A method as recited in claim 20, wherein the particular value comprises a duplicate of at least a portion of part of the plaintext message.

22. (Original) A method as recited in claim 20, wherein the curve comprises a hyperelliptic curve.

23. (Original) A method as recited in claim 20, wherein the recovering comprises:

decompressing the encrypted product identifier to obtain a decompressed value;

raising the decompressed value to a particular exponent to obtain a resulting value, wherein the raising is based at least in part on the size of the group of points on the Jacobian of the curve; and

converting the resulting value to a number having a particular number of bits, wherein the number comprises the plaintext message.

24. (Original) A method as recited in claim 20, wherein the particular value comprises a particular pattern.

25. (Original) A method as recited in claim 20, further comprising:

allowing a software product associated with the encrypted product identifier to be installed only if the encrypted product identifier is determined to be valid.

26. (Original) A method as recited in claim 20, further comprising:

checking a numeric value embedded in the plaintext message; and

determining, based on the numeric value, whether the encrypted product identifier corresponds to an authentic copy of a product

27. (Original) A method as recited in claim 20, further comprising:

comparing the numeric value to a record of numeric values; and

determining that the encrypted product identifier corresponds to an authentic copy of the product if the number value is included in the record of number values, and otherwise determining that the encrypted product identifier does not correspond to an authentic copy of the product.

28. (Currently amended) ~~An~~ A computer-implemented encryption method, comprising:

encrypting a message using a secret; and

wherein the secret comprises the order of a group of points on the Jacobian.

29. (Original) An encryption method as recited in claim 28, wherein the encrypting comprises:

receiving the message;

padding the received message using a recognizable pattern;

converting the padded message to a number represented by a particular number of bits;

converting the number to an element of the Jacobian of a curve;

raising the element to a particular power;

compressing the result of raising the element to the particular power; and

outputting, as an encrypted message, the compressed result.

30. (Original) An encryption method as recited in claim 28, wherein the Jacobian comprises a Jacobian of a hyperelliptic curve.

31. (Original) An encryption method as recited in claim 28, wherein the secret comprises the order of a group of points on the Jacobian of a curve, wherein the curve is given by the equation $y^2=f(x)$, wherein $f(x)$ has a degree of $2 \cdot g+1$, and wherein g refers to the genus of the curve.

32. (Original) An encryption method as recited in claim 28, wherein the message comprises a numeric value corresponding to a copy of a product, and wherein the encrypting creates a ciphertext that is a product identifier corresponding to the copy of the product.

33. (Original) An encryption method as recited in claim 32, wherein the numeric value corresponds to only one copy of the product.

34. (Currently amended) A computer-implemented decryption method, comprising:

decrypting a message using a secret; and

wherein the secret comprises the order of a group of points on a Jacobian of a curve.

35. (Original) A decryption method as recited in claim 34, wherein the curve comprises a hyperelliptic curve.

36. (Original) A decryption method as recited in claim 34, further comprising:

recovering a portion of the decrypted message;

checking whether the portion of the decrypted message corresponds to a particular product; and

determining that authentication of the particular product succeeds if the portion of the decrypted message corresponds to the particular product, and otherwise determining that authentication of the particular product fails.

37. (Original) A decryption method as recited in claim 34, wherein the message comprises a product identifier corresponding to a copy of a product.

38. (Original) A decryption method as recited in claim 34, wherein decrypting the message comprises:

decompressing the message to obtain a decompressed value;

raising the decompressed value to a particular exponent to obtain a resulting value, wherein the raising is based at least in part on the order of the group of points on the Jacobian of the curve; and

converting the resulting value to a number having a particular number of bits.

39. (Currently amended) A decryption method as recited in claim 38, further comprising:

checking whether a set of bits of the particular number of bits represents a recognizable pattern; and

determining that the ~~product identifier~~ number is valid if the set of bits do represent the recognizable pattern, and otherwise determining that the ~~product identifier~~ number is invalid.

40. (Currently amended) A system comprising:

an input module to receive a plaintext message to be encrypted; and

an encryption module, communicatively coupled to the input module, to convert the plaintext message to ciphertext based on both a curve and a secret that is the order of a group of points on a Jacobian of the curve.

41. (Original) A system as recited in claim 40, wherein the system further comprises:

a curve selection module, communicatively coupled to the encryption module, configured to select the curve and the Jacobian of the curve base at least in part on a set of input parameters.

42. (Original) A system as recited in claim 41, wherein the input parameters include both a genus of the curve and the order of a Jacobian of the curve.

43. (Original) A system as recited in claim 40, wherein the curve comprises a hyperelliptic curve.

44. (Original) A system as recited in claim 40, wherein the encryption module is configured to convert the plaintext message to ciphertext by:

padding the plaintext message using a recognizable pattern;

converting the padded message to a number represented by a particular number of bits;

converting the number to an element of the Jacobian of the curve, wherein the converting is based at least in part on the group of points on the Jacobian of the curve;

raising the element to a particular power; and

outputting, as the ciphertext, the result of raising the element to the particular power.

45. (Currently amended) A system comprising:

an input module to receive a ciphertext; and

a decryption module, communicatively coupled to the input module, to convert the ciphertext to a plaintext message based on both a curve and a secret that is the order of a group of points on a Jacobian of the curve.

46. (Original) A system as recited in claim 45, wherein the curve comprises a hyperelliptic curve.

47. (Original) A system as recited in claim 45, wherein the decryption module is configured to convert the ciphertext to a plaintext message by:

decompressing the ciphertext to obtain a decompressed value;

raising the decompressed value to a particular exponent to obtain a resulting value, wherein the raising is based at least in part on the order of the group of points on the Jacobian of the curve;

converting the resulting value to a number having a particular number of bits;

selecting a portion of the resulting value; and

using, as the plaintext message, the selected portion of the resulting value.